L-EGS7 - Security Confidence Test - LaRC DAAC

Overview

EGS LDAAC security architecture must meet the requirements for data integrity, tamper-proofing (for data integrity), encryption (for privacy), availability, confidentiality, authentication and authorization services. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. While authentication should always be used in every instance between client and server, the mechanisms for authorization, data integrity and privacy are based on security policies of the system(s) and the application-specific need for those mechanisms. Authentication is the process of verifying the validity of a principal. Authentication is usually done at two points. Initially when users log-in to the EGS domain, authentication is done by a "trusted third party" who supplies server's credentials for principals to use with application servers. Authorization is the process of deciding what sort of users/groups should be allowed to access what services /resources and then allow/deny the service. In authorization, each resource is associated with a list of permissions that should be granted to different user and different kinds of access operations. This is used to selectively grant certain principals access to specific resources. Authorization is performed by Access Control List (ACL) mechanism. An ACL is an entry with information such as the name of the user/group and the permissions list associated with them. Which indicates the kind of permissions given for the user/group. ACLs should be created and maintained for all the application specific objects.

Several FREEWARE products provide tools for authentication and network and system monitoring: Kerberos, SATAN, Crack, anlpassword, Secure Shell, TCP Wrapper, and Tripwire. The Open Software Foundation's Distributed Computing Environment (OSF/DCE) employs Kerberos for authenticating user requests for network services. The FREEWARE product, SATAN, monitors networks and finds system security vulnerabilities. Three FREEWARE products — Crack, nlpassword and Secure Shell — provide additional password protection for local system and network access. To monitor and control access to network services, ECS Security Services uses TCP Wrapper. The Tripwire monitors changes to files and flags any unauthorized changes. Security Services also supports detection of, reporting, and recovery from security breaches. Security logs should be monitored and security reports generated should be reviewed periodically to verify whether the EGS security services meet LDAAC security policies and procedures.

When data is transmitted over the network from one application to another, the integrity of the data should be preserved. This is to make sure that the copy of the data the receiver gets is exactly the same as the data that the sender sends. This tamper-proofing of the data may or may not be used with methods for protecting the privacy of the data. Checksums or secure hashes are often used to guarantee data integrity. Encryption is the process of encoding a message into cipher text using a key. The process of decoding the

cipher text to its original form using a key is called decryption is used to maintain the privacy of data transmitting over the network. Authentication is necessary, other features; authorization, checksums and data privacy are optional. EGS LDAAC application can selectively choose to use these security features depending on their specific needs.

Test Objectives:

Test Case 1: EGS Physical Security
The objective of this test is demonstrate EGS security capability to:

- provide Physical Security for protective measure against access control to the logical and physical EOSDIS system.
- protect system components and data from unauthorized access.

Test Case 2: EGS Science Data Access Controls
The objective of this test is to demonstrate EGS security capability to:

- confirm authentication, and identification of individual user.
- control user access and prevention of data compromise and/or corruption resulting from unauthorized access.

Test Case 3: Virus Detection
The objective of this test is demonstrate EGS security capability to:

- detect computer software system viruses and worms.
- Contain or destroy a viruses and worms.

Test Case 4: Security Monitoring and Auditing
The objective of this test is demonstrate EGS security capability to:

- provide automatic alert for intrusion events.
- perform intrusion detection check in order to maintain the integrity of ECS resources.

Test Case 5: Audit Trails
The objective of this test is demonstrate EGS security capability to:

- provide the capability to analyze security audit trail.
- provide the mechanism to generate security activities report.

Requirements Verified:

This section specifies the overall EGS security requirements as applicable to all EGS elements. The LDAAC will have primary responsibility for EGS security management services relevant to LDAAC. The SMC will have overall responsibility for implementation, maintenance and monitoring of EGS security management services at LDAAC. In the following requirements, security controlled data are those that have limited access and security protection constraints.

EOSD2400#B	EOSD2430#B	EOSD2440#B	EOSD2480#B
EOSD2510#B	EOSD2550#B	EOSD2555#B	EOSD2620#B
EOSD2640#B	EOSD2650#B	EOSD2660#B	EOSD2710#B

EOSD2990#B	EOSD3000#B	EOSD3200#B	EOSD3220#B
ESN-0010#B	ESN-0590#B	ESN-0600#B	ESN-0650#B
ESN-1360#B	ESN-1365#B	ESN-1380#B	ESN-1400#B
ESN-1430#B	IMS-0060#B	IMS-0230#B	IMS-1630#B
SMC-2105#B	SMC-5305#B	SMC-5325#B	SMC-5335#B
SMC-5345#B	SMC-5355#B	SMC-5365#B	SMC-6315#B
SMC-6325#B			

Test Configuration:

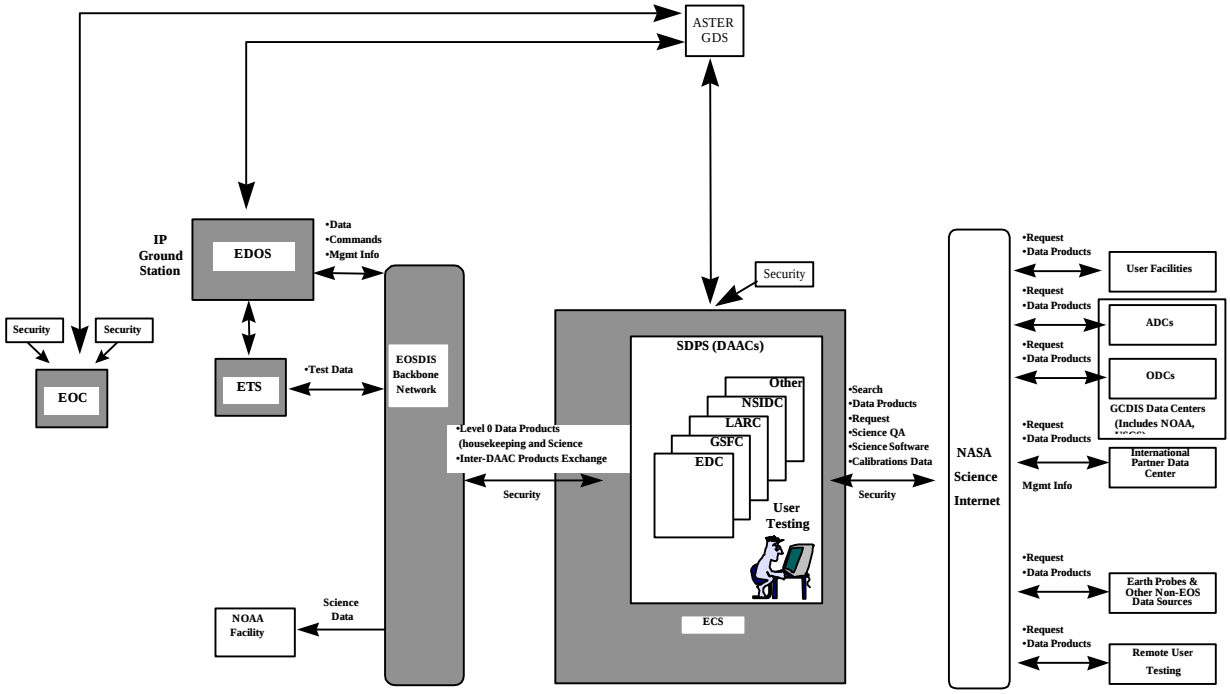

Figure 7.1 Security Test Configuration

Participants and Supporting Requirements:

Participanting Organizations:

M & O Support at LaRC DAAC

Communication support:

Voice – CCL or direct phone line to system personnel
Data – EBNet WAN Routers and associated hardware

NSI for General Users
IP address: Release B) IMS ; Xwindow GUI's, PC

Equipment and Software:

Software: Release B.0 Client Software configured on each workstation Desktop PC's, email, Browsers, FTP Software, DCE, and Tivoli

Hardware: Xterms, X-Window GUI's, Servers: Real-time Server, Data Server, Multicast Server, Data Storage Unit (File Servers, RAID Units), EOC Workstations

Test Tools:

CRACK - Ensures password integrity.
ANLpassword - provides additional password protection for local system and network access.
SATAN - monitors network and system security vulnerabilities.
Tripwire - monitors changes to files and flags any unauthorized changes.
TCP Wrapper - monitors and filters incoming request for network services.
Kerberos and Access Control Lists (ACL) - authenticates users.

Test Data:

TBD

Test Case Description:

For certification purpose, the following procedure is used to verify the security functionalities (such as, Physical Security, Access Controls, Identification, Authentication, Network Security, Security Software, Security Monitoring and Auditing), at LDAAC.

The test cases and procedures will be finalized after discussions with LDAAC and other participants.

L-EGS7.01 EGS Physical Security

Test Objective

This test verifies that EGS security services are in compliance with the applicable Federal and NASA guidelines, i.e. NHB 1620.3, "NASA Security Handbook." The method of verification includes inspection of related documents and handbooks. All EOSDIS Elements (DAAC's, SMC, DOA, EOC, etc.) shall take protective measures that control access to the EOSDIS system including system access (such as remote login, telnet, ftp, network browser etc), hardware (such as removable media, terminals, printers etc) and software (such as database, configuration management system etc). These protective measures include the network authentication service,

monitoring network vulnerabilities, password integrity and monitoring requests for network services. All computer equipment used by EOSDIS elements should be located in a controlled facility thatmeets environmental and accounting procedures. Access to the system console should be restricted to the computer system operational staff. All the system level activities should be conducted in secured environment. System users unsecured locations should be log off from the system when it is not in use

Requirements to be Verified:

EOSD2640#B EOSD3000#B EOSD3200#B EOSD3220#B SMC-5305#B

Test Procedures:

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
1.001	LaRC DAAC	Verify that computer room has locked or combination locked door(s).	The locked door(s) or combination door(s) are present and in working condition.			
2.001	LaRC DAAC	Verify that environmental temperature controls exit check to see if it is working properly within the computer room.	Separate thermostat, fire extinguisher, smoke detectors and/or separate air conditioner unit in working condition.			
2.002	LaRC DAAC	Verify that Security Audit trails, logs and backup tapes or disks for ECS software and key data items exist.	Security Audit trails, Backup label and log book are current; Mounted tape or disk show ECS software and key data items are present.			
2.003	LaRC DAAC	Verify backup media and Security audit trails and logs are stored in a separate area.	Backup media, audit trails and logs are stored in a separate office or building.			

L-EGS7.02 ECS Science Data Access Control

Test Objective

This test verifies the DAAC's ability to control user access and prevention of data corruption resulting from unauthorized access. This test is used to verify that all EOSDIS elements have implemented access controls commensurate with sensitivity level 2 requirements as outlined in

NHB 2410.9A (Chapter 4). Access control shall include procedural and computer security protective measures that facilitate the management to identify unauthorized access to EOSDIS system resources. All access to EOSDIS billable data and services shall be protected with at least sensitivity level 2 measures. All EOSDIS element users with access to sensitive resources shall be uniquely identified through an individual account. If there is a need for user group accounts, these accounts shall be approved in advance by EOSDIS management services. A procedure shall be in place for the creation of new accounts and the removal of accounts no longer needed. The procedure for removing defunct accounts should be conductedaccording to the guidelines set by SMC. In addition, all users with access to sensitive resources shall have specified restrictive functional capabilities. This test also verifies that all DAACs shall provide a warning banner that indicates the user's actions may be monitored. The banner content is checked to verify not to contain any type of information about the system (e.g., type of operating system, version level etc.,), or providing HELP information until after the user has successfully logged into the system and the user login information has been authenticated.

Access Control Level 2 Protection measures would include:

- Identification and authentication of individual users.
- Restriction of functional capabilities of individual users.
- Users access control to the data and applications.
- Data encryption.

Requirements to be verified:

EOSD2400#B	EOSD2430#B	EOSD2440#B	EOSD2480#B
EOSD2550#B	EOSD2555#B	EOSD2620#B	ESN-0010#B
ESN-1360#B	ESN-1380#B	ESN-1400#B	IMS-0060#B
IMS-0230#B	IMS-1630#B	SMC-2105#B	SMC-5325#B
SMC-5335#B	SMC-5365#B		

Test Procedures:

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
1.001	LaRC DAAC	Logs-in as a security administrator user using a valid username and password.	Log-in allowed and the system displays security administrators main menu.			3/5/97
1.002	LaRC DAAC	Verify the existence of virus detection software.	The virus detection software is installed and operational on the system.			
2.001	LaRC DAAC	Performs create, change and delete commands to the security registry.	User accounts are created, changed and deleted.			
2.002	LaRC DAAC	Verifies that the user accounts contain username, password, group and user identification code, login directory and command line interpreter.	User accounts reflect create, change and delete commands entered.			
2.003	LaRC DAAC	Logs off.	The ECS login screen is displayed on the screen.			
2.004	LaRC DAAC	Using SATAN and CRACK, attempt to login by guessing user id and related passwords. Repeat multiple times.	The security management service detects the multiple events after the pre-established threshold. The service sends notification of security alert to the Computer Operator.			
2.005	LaRC DAAC	The Computer Operator receives multiple security alerts and begins to investigate the cause of alerts by invoking the events browser (log) to retrieve the security events.	The event browser displays the requested events. The information should contain the following: a. Data and time of the event b. User name c. Type of event d. Success or failure of			

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
			the event e. Origin of the request.			
2.006	LaRC DAAC	Discovers that the login attempts on the multiple hosts originated from the same area. The Operator contacts the MIS manager at the location of the User (Hacker) proceeds to have the issue investigated locally. The Operator sends email to all ECS sites informing them of the event and to explicitly deny access from this area.	All EGS sites receive the email.			
2.007	LaRC DAAC	The operator modifies the network security authorization data bases to deny all incoming accesses from the host in question.	Network security authorization databases deny all incoming accesses from the host in question.			
2.008	LaRC DAAC	Using the 1st authorized/approved user account, log-in to ECS using a valid user id and password.	The user is able to log onto the system. The next user screen appears.			
2.009	LaRC DAAC	Using a network analyzer, verify that the password is not readable over the network.	The pass is not readable over the network.			
2.010	LaRC DAAC	Using the 2nd authorized/approved user account, attempt log onto the EGS using the same valid user id and password used by the 1st	The user is unable to log onto the system. A message indicating the user is already logged on is displayed.			

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
		authorized/approved User in step 2.004.				
2.011	LaRC DAAC	Using the 1st authorized/approved user account, compromise the data by deleting the access control file.	The system detects the compromise, isolates it, until it can be eliminated.			
2.012	LaRC DAAC	The Operator discovers the security violation compromise. Using the Office Automation tools provided, generates instructions for recovery from the detected security event.	Instructions for the recovery from the detected security event are generated.			
		Invalid Remote Login				
2.013	LaRC DAAC	Attempt to remote login to the ECS using an invalid password.	The login attempt is denied.			
2.014	LaRC DAAC	Remote login using valid user id and password .	Login allowed.			
2.015	LaRC DAAC	Remote user attempts to access restricted directories (TBD), local files (TBD), services (TBD), and commands (TBD) for remote access.	Access denied.			
2.016	LaRC DAAC	Attempt to access restricted data (Restricted Data TBD) using a valid username and a invalid password.	Access is denied.			
2.017	LaRC DAAC	Attempt to access restricted data (Restricted Data TBD) using a valid group name and a invalid password.	Access is denied.			
2.018	LaRC DAAC	Attempt to access restricted data	Access is denied.			

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
		(Restricted Data TBD) using a invalid group name and a valid password.				
2.019	LaRC DAAC	Attempt to update restricted data using a valid username and a invalid password.	Attempt to update privileges will be denied.			
2.020	LaRC DAAC	Attempt to update restricted data using a valid username and a valid password.	Update permitted.			
2.021	LaRC DAAC	Attempt to update restricted data using a valid group name and a invalid password.	Update denied.			
2.022		Review audit logs to verify that current activities were captured.	Audit logs should be displayed and analyzed.			
3.001	LaRC DAAC	Exit and close functions.	All functions are closed.			
3.002	LaRC DAAC	Log off of the system.	The system displays the login screen.			

L-EGS7.03 Virus Detection

Test Objective

This test verifies that the EGS detects attempt to ingest information which contains virus and /or worms. A user logs into the system using a PC. While logged onto the system, the user attempts to push a document onto the system which contains a virus. The system should detect the virus and alert system personnel. A virus is also attached to mail message and attempt to enter the system. The system should detect the corrupted attachment and alert the operators.

Requirements to be verified:

EOSD2510#B SMC-5345#B

Test Procedures:

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
1.001	LaRC DAAC	Logon as the Security Administrator on the Security Monitoring Console.	Log-in allowed and the system displays the main menu.			
2.001	LaRC DAAC	Verify that existence of virus detection software.	The virus detection software is installed and operational.			
2.002	LaRC DAAC	Logon as an ECS user.	Login allowed.			
2.003	LaRC DAAC	Attempt to push a document that contains a virus.	Transfer of Document begins.			
2.004	LaRC DAAC	Monitor Security Console for an alert.	An Alert at the Security Console appears indicating that a virus has been detected.			
2.005	LaRC DAAC	Virus Detection Software destroys the virus.	A prompt on the Console appears indicating that virus has been successfully removed.			
2.006		System Administrator takes further action to ensure that the virus is contained.				
3.001	LaRC DAAC	Logoff of the system.	Login window is displayed.			

L-EGS7.04 Security Monitoring and Auditing

Test Objective

This test verifies that the LaRC DAAC security management services periodically checks the network the EOSDIS interfaces to verify its proper operational status and to detect all unaccountable deviation to its operational policies. This test verifies that system auditing will contain, at a minimum, review of all break-in attempts, accesses from inactive and detached processes, modifications to user authorization files, and remote access. Audit logs should be analyzed and retained for specified period of time.

Requirements to be verified:

EOSD2510#B	EOSD2660#B	ESN-0650#B	ESN-1380#B
ESN-1430#B	SMC-5335#B	SMC-5355#B	SMC-5365#B
SMC-6315#B	SMC-6325#B		

Test Procedures:

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
1.001	LaRC DAAC	Logs-in as a security administrator user using a valid username and password.	Log-in allowed and the system displays security administrators main menu.			3/5/97
2.001	LaRC DAAC	**For more detailed test procedures, refer to Section 5.3 of the 611 document.**				

L-EGS7.05 Audit Trails

Test Objective

This test verifies that all the information required for audit trail is being maintained. Reports are generated and its content verified. System backups are verified to include audit trails. Security policies are also inspected.

Requirements to be verified:

EOSD2510#B	EOSD2650#B	EOSD2710#B	EOSD3200#B
ESN-0650#B	ESN-1430#B	SMC-5305#B	SMC-5345#B
SMC-6315#B	SMC-6325#B		

Test Procedures:

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
1.001	LaRC DAAC	Log-in as the System Administrator.	Log-in successful			
2.001	LaRC DAAC	Type the following command to initialize the audit subsystem **"/etc/security/audit_startup"**.	The audit subsystem is initialized.			
2.002	LaRC	To close the current	The current audit file is			

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
	DAAC	audit file and open a new audit file in the current audit directory, type the following command **"audit -n".**	closed and a new audit file is opened.			
2.003	LaRC DAAC	To read the current audit file, type the following command **"audit -s".**	The file is read and stored internally. The audit information should contain the following: a. Date and time of the event, b. User Name, c. Type of event, and d. Origin of request.			
2.004	LaRC DAAC	To close the current audit file, type the following command **"audit -t".**	The audit file is disabled.			
2.005	LaRC DAAC	To display the audit output, type the following command **"praudit -sl *filename*".**	The audit output is displayed.			
2.006	LaRC DAAC	Confirm all logon attempts from previous testing are recorded in audit logs and have restricted access.				
2.007	LaRC DAAC	Confirm all object, resources and subject access denials are recorded and have restricted access.				
2.008	LaRC DAAC	Confirm all accesses to privileged systems are recorded and have restricted access.				
2.009	LaRC DAAC	Confirm all accesses to the ESDIS systems are recorded and have restricted access.				

Step ID	Station	Actions	Results	Comments	Verified Reqs.	Last Modified
2.010	LaRC DAAC	Confirm that there is a inventory accounting system in place to record all media entering and leaving facility.				
2.011	LaRC DAAC	Confirm that there is at least one generation of backup applications software stored off-site and it is retrievable in a timely manner.				
2.012	LaRC DAAC	Generate a daily backup.	Confirm that data created is saved and retrievable from physical media and is restorable to that backup to Ensure accuracy.			
2.013	LaRC DAAC	Generate a monthly backup.	Confirm that data created is saved and retrievable from physical media.			
2.014	LaRC DAAC	Generate a full system weekly backup.	Confirm that data created is saved and retrievable from physical media and is restorable to that backup to Ensure accuracy.			
2.015	LaRC DAAC	Generate a full system monthly backup.	Confirm that data created is saved and retrievable from physical media.			
2.016	LaRC DAAC	Ensure that software backup copies are stored off site and readily accessible in a timely manner.				
2.017	LaRC DAAC	Note times and steps required to access off site software.				

Appendix: Test Package Requirements Summary

Requirement	Description	Test Case(s)
EOSD2400#B	ECS shall provide multiple categories of data protection based on the sensitivity levels of ECS data, as defined in NHB 2410.9.	
EOSD2430#B	Data base access and manipulation shall accommodate control of user access and update of security controlled data.	
EOSD2440#B	Data base integrity including prevention of data loss and corruption shall be maintained.	
EOSD2480#B	ECS elements shall require unique sessions when security controlled data are being manipulated.	
EOSD2510#B	ECS elements shall maintain an audit trail of: a. All accesses to the element security controlled data b. Users/processes/elements requesting access to element security controlled data c. Data access/manipulation operations performed on security controlled data d. Date and time of access to security controlled data e. Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes f. Detected computer system viruses and worms g. Actions taken to contain or destroy a virus	
EOSD2550#B	The ECS elements shall limit use of master passwords or use of a single password for large organizations requiring access to a mix of security controlled and non-sensitive data.	
EOSD2555#B	ECS shall maintain confidentiality of user product request and accounts.	
EOSD2620#B	ECS elements shall disconnect a user/element after a predetermined number of unsuccessful attempts to access data.	
EOSD2640#B	ECS elements shall relinquish a connection between the element and a user when the user has not been active for a configurable period of time.	
EOSD2650#B	ECS elements shall report detected security violations to the SMC.	
EOSD2660#B	ECS elements shall at all times maintain and comply with the security directives issued by the SMC.	
EOSD2710#B	ECS elements shall report all detected computer viruses and actions taken to the SMC.	
EOSD2990#B	The ECS elements shall support the recovery from a system failure due to a loss in the integrity of the ECS data or a catastrophic violation of the security	

	system.	
EOSD3000#B	The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup.	
EOSD3200#B	A minimum of one backup which is maintained in a separate physical location (i.e., different building) shall be maintained for ECS software and key data items (including security audit trails and logs).	
EOSD3220#B	All media shall be handled and stored in protected areas with environmental and accounting procedures applied.	
ESN-0010#B	ESN shall provide the following standard services: a. Data Transfer and Management Services b. Electronic Messaging Service c. Remote Terminal Service d. Process to Process Communication Service e. Directory and User Access Control Service f. Network Management Service g. Network Security and Access Control Service h. Internetwork Interface Services i. Bulletin Board Service	
ESN-0650#B	The ESN shall perform the following network management functions for each protocol stack implemented in any ECS element, and each communications facility: a. Network Configuration Management b. Network Fault Management c. Network Performance Management d. Network Security Management	
ESN-1360#B	The ESN shall control access of processes and users through an authentication and authorization service that meets GNMP standards.	
ESN-1365#B	The ESN shall isolate FOS with secure interfaces.	
ESN-1380#B	The ESN shall provide countermeasures for the following security threats related to data communications: a. modification of data (i.e., manipulation) while in transit over the network b. disclosure of authentication information c. degradation in network or processing resource performance through denial of service attack d. Impersonation of authentication credentials or authorization privileges.	
ESN-1400#B	The following security functions and services, at a minimum, shall be provided: a. authentication b. access (authorization) control	

	c. data integrity d. data confidentiality	
ESN-1430#B	The ESN shall provide the following security event functions: a. Event detection b. Event reporting c. Event logging	
IMS-0060#B	The IMS shall restrict update of ECS directory, inventory, and guide (documentation/reference material) and other IMS data bases to authorized users based on the users access privileges.	
IMS-0230#B	The IMS shall restrict update of ECS directory, inventory, and guide (documentation/reference material) and other IMS data bases to authorized users based on the users access privileges.	
IMS-1630#B	The IMS shall provide the capability to receive from the SMC, directives to include at a minimum: a. Directives for integration, testing, and simulation b. Maintenance directives c. Configuration management directives d. Logistics management directives e. Training management directives f. Fault management directives g. Security directives	
SMC-2105#B	The LSM shall convey ground operations (i.e., non-instrument related) events to sites or elements for implementation. Ground operations events include, at a minimum, actions associated with: a. Configuring element resources b. Fault recovery c. Security d. Maintenance e. Testing f. Simulations g. Logistics h. Training classes i. Accounting and accountability j. General requests for information	
SMC-5305#B	The LSM shall maintain security policies and procedures, including, at a minimum: a. Physical security b. Password management c. Operational security d. Data classifications e. Access/privileges f. Compromise mitigation	

SMC-5325#B	The LSM shall promulgate, maintain, authenticate, and monitor user and device accesses and privileges.	
SMC-5335#B	The LSM shall perform security testing that includes, at a minimum, password auditing and element internal access/privileges checking.	
SMC-5345#B	The LSM shall perform compromise (e.g., virus or worm penetration) risk analysis, and detection.	
SMC-5355#B	The LSM shall isolate the compromised area, detach the compromised input I/O, and the compromised areas output I/O until the compromise has been eliminated.	
SMC-5365#B	The LSM shall generate recovery actions in response to the detection of compromises.	
SMC-6315#B	The LSM shall perform, as needed, security audit trails within its element.	
SMC-6325#B	The LSM shall perform, as needed, data and user audit trails within its element.	